Systems and Internet Infrastructure Security

Network and Security Research Center
Department of Computer Science and Engineering
Pennsylvania State University, University Park PA

HECURA: Exploiting Asymmetry in Performance and Security Requirements for I/O in High-end Computing

Patrick McDaniel and Anand Sivasubramaniam

HECIWG FSIO 2007 Workshop
Arlington, VA -- August 6th, 2007

E.g.: High-Performance Grid

- The first 5 minutes of processing atmospheric data received from remote instruments represents an order of magnitude reduction in data volume ....
  - Terabytes of data
  - Short lifetimes
  - Integrity is paramount
  - Experimenters trusted

Q: *How do you tune the data collection and application to process this much data efficiently and securely?*

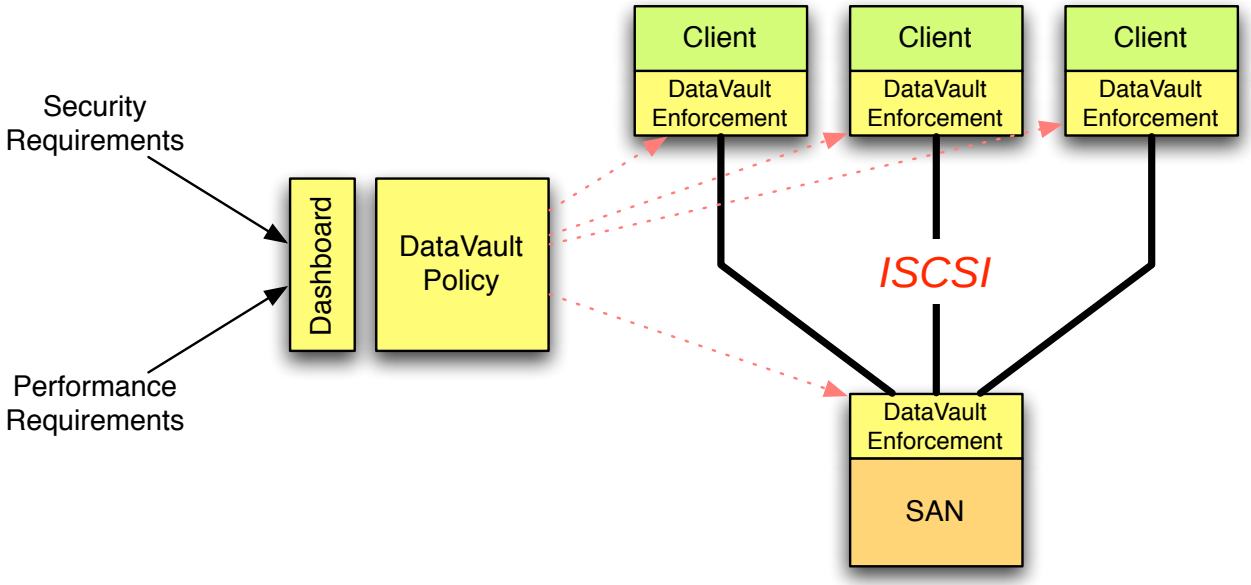
Storage Challenges

PENNSTATE 1855

- Storage in high-end computing environments faces:
  - Each *environment* has unique security requirements
  - Each *data type* may warrant different mechanisms
  - Each *application* has different performance/security tolerances
  - Each *storage architecture* has different price/performance
- Thus, a high-end deployment represents a complex and constantly evolving performance and security tradeoff.
- Reality: current storage systems fail to assess and implement complex a storage calculus
  - *Security and performance are not orthogonal concerns*
- *Problem*: security necessarily introduced on critical I/O path

DataVault

- *DataVault*: a runtime configurable storage system



- *Optimization*: find protocol behaviors and enhancements that meet security and performance profile: *policy*
  - lazy encryption, deferred authentication, deferred access control
- Target: Cluster Systems and SANs

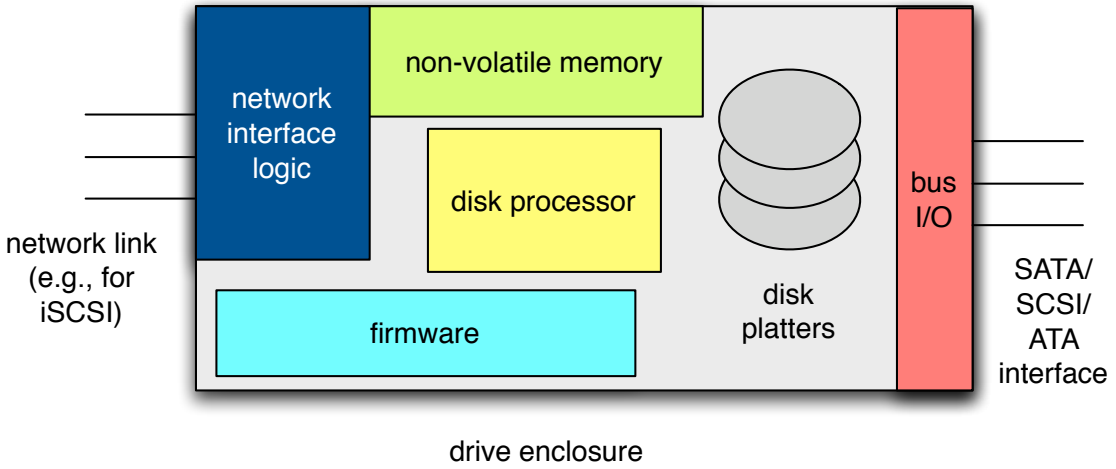
Research Threads

PENNSTATE 1855

- Policy Architectures/enforcement: meeting security requirements and solutions for next generation storage
  - Architecture/hardware enhancements
  - Security policies, specifications
  - Cryptographic constructions
- Performance: evaluating performance optimizations in storage systems
  - Architecture enhancements
  - Protocol Improvements
  - Cryptographic constructions

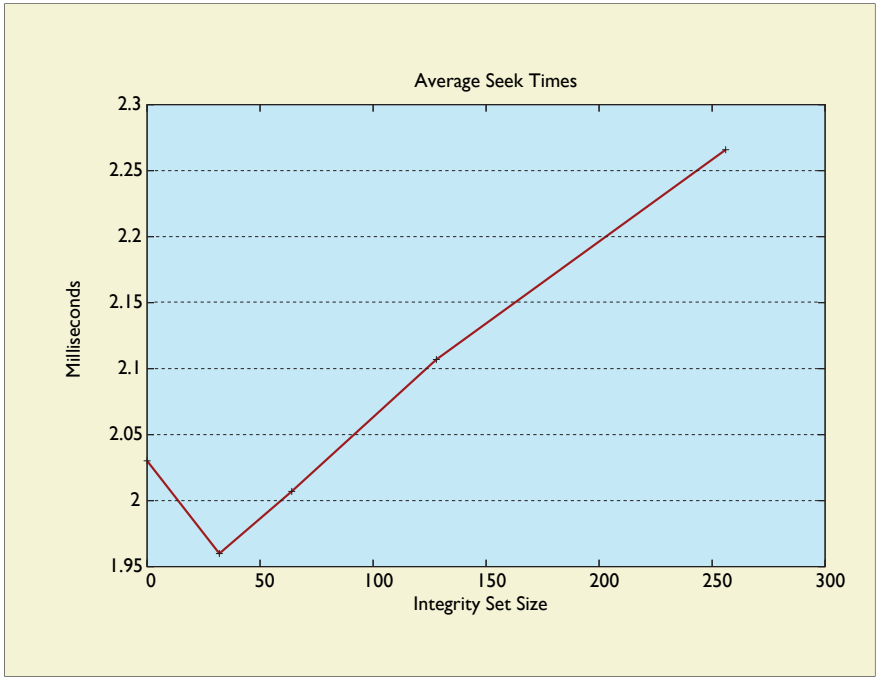
Security Policy Architectures

- New storage architectures can be used to implement *security policy* enforcing services at the disk layer
- *Hybrid hard drives* combine spinning disk platters with non-volatile memory banks within drive enclosure
- *Vision*: use NVRAM as a repository for security metadata along with on-disk processing capabilities to allow for storage-level policy enforcement



Security Policy Architectures

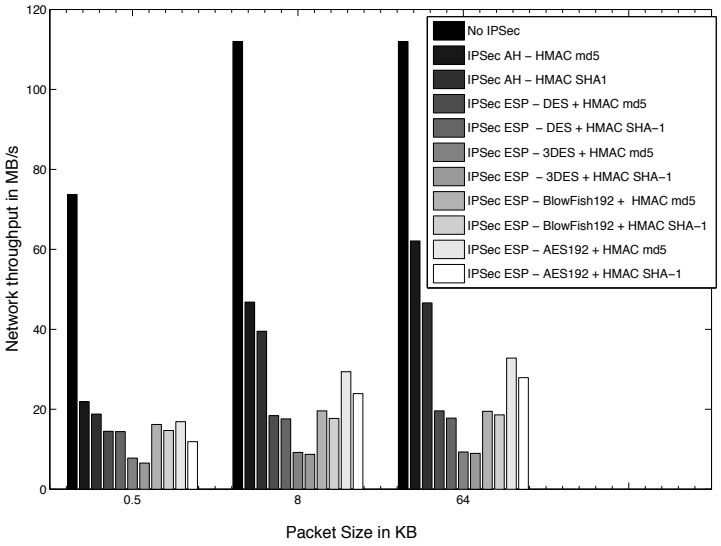
- Applications
  - authenticated encryption
  - capability systems
  - information flow
- *Integrity sets* trade off NVRAM storage for disk performance



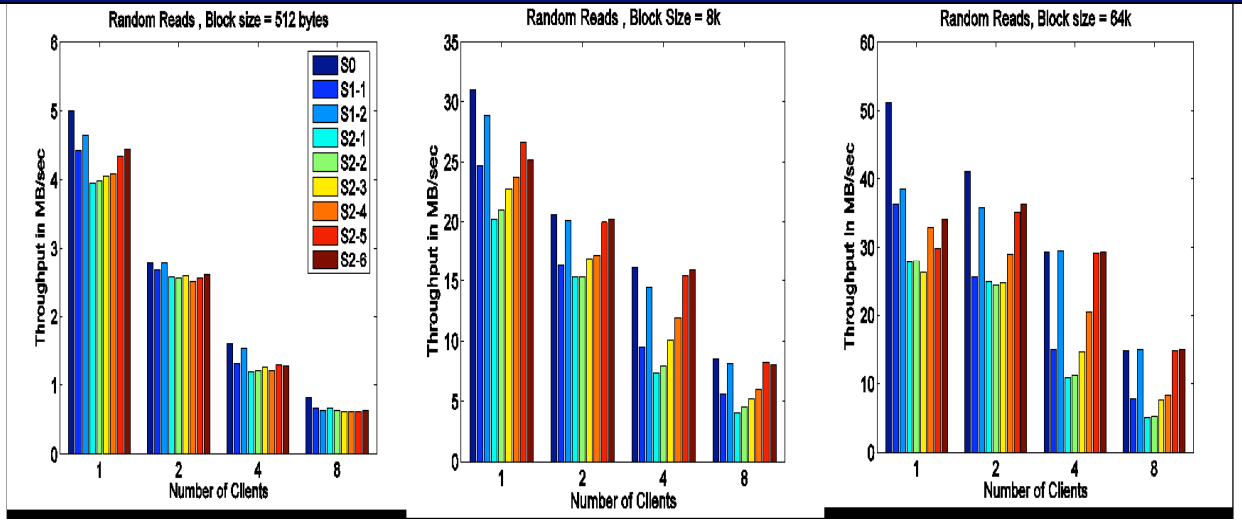
  - performance is helped by spatial locality of information on disks
  - Updates become more efficient as file sizes get larger (e.g., small portion of 2 GB file changes, only that portion needs recalculation rather than the entire file)
- Preliminary publication: Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. Non-Volatile Memory and Disks: Avenues for Policy Architectures. First Computer Security Architecture Workshop (CSAW 2007), November 2007.

Optimizing Security

- *iSCSI* relies on *IPsec* to provide transport security, which exacerbates packet processing overheads
- Linux 2.6, 3Ghz intel: for 8 KB pkt AH degrades network throughput by 58%, ESP degrades by 74%
- *Bottleneck*: crypto, then TCP
  - IPsec unaware of caching behavior
- Solution: lazy mechanisms
  - *lazy decryption*: store encrypted data on server, only clients decrypt (move conf. to iSCSI layer, use IKE for key mgmt.)
  - *lazy authentication*: delay authentication and perform operations at client (N.B.: in both cases, headers are immediately processed)



Performance Tradeoffs



- smaller block sizes dominated by network processing, larger block sizes dominated by crypto processing
- lazy approaches outperform IPsec with a performance increase of 30-40% over ESP for large block sizes, depending on workloads (*rawio, BTIO, dbench*)

- Preliminary publication: S. Chaitanya, K. Butler, A. Sivasubramaniam, P. McDaniel, and M. Vilayannur. Design, implementation and evaluation of security in iSCSI-based network storage systems. 2nd International Workshop on Storage Security and Survivability, 2006.

Summary

- Addressing security and performance of HEC:
  - Exploiting behavior of protocols can allow crypto optimizations
  - Lazy security: Scalability leveraging endpoints to offset costs
  - New cryptographic constructions: ABE, IBE, new modes
  - Policy specification: how to express security requirements
- Future: detailed simulation and experimentation will provide better understanding of tradeoffs and challenges, and lead to generalizations ...
  - Disksim, further experiment NVRAM extensions
  - Direct measurement (iSCSI, others..), applications ...
  - DataVault: new optimizations, interfaces, schedulers

Other Project Details

- Faculty Funded
  - Patrick McDaniel
  - Anand Sivasubramaniam
- Students Funded
  - Kevin Butler, PSU
  - Shiva Chaitanya, PSU
- Collaborations
  - Trent Jaeger, PSU
  - Bhuvan Urgaonkar, PSU
- Issuses: none

Publications

PENNSTATE 1855

- Other Related Publications:
  - William Enck, Patrick McDaniel, Shubho Sen, Panagiotis Sebos, Sylke Spoerel, Albert Greenberg, Sanjay Rao, and William Aiello. Configuration Management at Massive Scale: System Design and Experience. Proceedings of the USENIX Annual Technical Conference, June 2007. Santa Clara, CA.
  - Boniface Hicks, Kiyan Ahmadizadeh, and Patrick McDaniel. Understanding Practical Application Development in Security-Typed Languages. 22st Annual Computer Security Applications Conference (ACSAC), pages 153--164, December 2006. Miami, Fl. (best student paper).
  - Boniface Hicks, Dave King, and Patrick McDaniel. Jifclipse: Development Tools for Security-Typed Applications. Proceedings of the 2nd ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS '07), June 2007. San Diego, CA.
  - Boniface Hicks, Sandra Rueda, Trent Jaeger, and Patrick McDaniel. Integration of SELinux and Security-typed Languages. Proceedings of the 2007 Security-Enhanced Linux Workshop, March 2007. Baltimore, MD.

Contact Info

PENNSTATE 1855

Contact: mcdaniel@cse.psu.edu

http://siis.cse.psu.edu/

http://www.cse.psu.edu/~emcc/